On the Existence of Perfect Codes for Asymmetric Limited-Magnitude Errors

Sarit Buzaglo
Dept. of Computer Science
Technion-Israel Institute of Technology
Haifa 32000, Israel
Email: sarahb@cs.technion.ac.il

Tuvi Etzion
Dept. of Computer Science
Technion-Israel Institute of Technology
Haifa 32000, Israel
Email: etzion@cs.technion.ac.il

***Abstract*—Block codes, which correct asymmetric errors with limited-magnitude, are studied. These codes have been applied recently for error correction in flash memories. The codes will be represented by lattices and the constructions will be based on a generalization of Sidon sequences. In particular we will consider perfect codes for these type of errors.**

I. Introduction

Asymmetric error-correcting codes were subject to extensive research due to their application in coding for computer memories [8]. The advance of technology and the appearance of new nonvolatile memories, such as flash memory, led to a new type of asymmetric errors which have limited-magnitude. A multilevel flash cell is electronically programmed into q threshold levels which can be viewed as elements of the set $\{0, 1, \ldots, q-1\}$. Errors in this model are usually in one direction and are not likely to exceed a certain limit. This means that a cell in level i can be raised by an error to level j, such that $i < j$ and $j-i \leq \ell$, where ℓ is the error limited-magnitude.

Asymmetric error-correcting codes with limited-magnitude were proposed in [1] and were first considered for nonvolatile memories in [2], [3]. Recently, several other papers have considered the problem, e.g. [4], [5], [6], [11].

In this work we mainly consider perfect codes for asymmetric limited-magnitude errors. We will consider only linear codes, unless otherwise is stated. Each t-error-correcting perfect code in the Hamming scheme, over GF(q), is also a perfect code for error-correction of t asymmetric errors with limited-magnitude $q-1$ [3]. Especially, a Hamming code of length $n = \frac{q^r-1}{q-1}$, over GF(q), can correct one asymmetric error with limited-magnitude $q-1$. Additional perfect codes for correction of one asymmetric error with limited-magnitude ℓ are obtained from tiling of $\mathbb{Z}^n$ with semi-crosses whose arms have length ℓ [10]. Perfect unbalanced limited-magnitude codes were considered in [9].

The rest of this work is organized as follows. In Section II we will define the basic concepts for codes which correct t asymmetric errors with limited-magnitude ℓ. We will show a convenient way to handle such codes and discuss three equivalent representations of such codes. In Section III we will present a new construction for perfect codes of length n which correct $n-1$ asymmetric errors with limited-magnitude ℓ, for any given ℓ. In Section IV we show that perfect codes of length n which correct $n-2$ asymmetric errors with limited-magnitude one cannot exist. We conclude in Section VI.

II. Basic Concepts

For a word $X = (x_1, x_2, \ldots, x_n) \in Q^n$, the *Hamming weight* of X, $w_H(X)$, is the number of nonzero entries in X, i.e., $w_H(X) = |\{i \ : \ x_i \neq 0\}|$.

A *code* $\mathcal{C}$ of *length* n over the alphabet $Q = \{0, 1, \ldots, q-1\}$ is a subset of Q^n. A vector $\mathcal{E} = (e_1, e_2, \ldots, e_n)$ is a t-*asymmetric-error with limited-magnitude* ℓ if $w_H(\mathcal{E}) \leq t$ and $0 \leq e_i \leq \ell$ for each $1 \leq i \leq n$. The sphere $\mathcal{S}(n, t, \ell)$ is the set of all t-asymmetric-errors with limited-magnitude ℓ. A code $\mathcal{C} \subseteq Q^n$ can correct t asymmetric errors with limited-magnitude ℓ if for any two codewords $X_1,\ X_2$, and any two t-asymmetric-errors with limited-magnitude ℓ, $\mathcal{E}_1,\ \mathcal{E}_2$, such that $X_1 + \mathcal{E}_1 \in Q^n$, we have that $X_1 + \mathcal{E}_1 \neq X_2 + \mathcal{E}_2$.

For simplicity it is more convenient to consider the code $\mathcal{C}$ as a subset of $\mathbb{Z}_q^n$, where all the additions are performed modulo q. Such a code $\mathcal{C}$ can be viewed also as a subset of $\mathbb{Z}^n$ formed by the set $\{X + qY \ : \ X \in \mathcal{C},\ Y \in \mathbb{Z}^n\}$.

We will represent a linear code $\mathcal{C}$, over $\mathbb{Z}_q^n$, which corrects t asymmetric errors with limited-magnitude ℓ, in two more different ways. The first is by an integer lattice and the second is by a generalization of the well-known Sidon sequence, the $\mathcal{B}_h$ sequence. We will show an equivalence between the three representations.

An *integer lattice* Λ is an additive subgroup of $\mathbb{Z}^n$. We will assume that

$$\Lambda \stackrel{\text{def}}{=} \{u_1\mathbf{v}_1 + u_2\mathbf{v}_2 + \cdots + u_n\mathbf{v}_n \ : \ u_1, u_2, \cdots, u_n \in \mathbb{Z}\}$$

where $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is a set of linearly independent vectors in $\mathbb{Z}^n$. The set of vectors $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ is called *the basis* for Λ, and the $n \times n$ matrix

$$\mathbf{G} \stackrel{\text{def}}{=} \begin{bmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \ldots & v_{nn} \end{bmatrix}$$

having these vectors as its rows is said to be the *generator matrix* for Λ.

The *volume* of a lattice Λ, denoted by $V(\Lambda)$, is inversely proportional to the number of lattice points per a unit volume. There is a simple expression for the volume of Λ, namely, $V(\Lambda) = |\det \mathbf{G}|$.

A set $P \subseteq \mathbb{Z}^n$ is a *packing* of $\mathbb{Z}^n$ with a shape $\mathcal{S}$ if copies of $\mathcal{S}$ placed on the points of P (in the same relative position) are disjoint. A set T is a *tiling* of $\mathbb{Z}^n$ if it is a packing and the

disjoint copies of $\mathcal{S}$ cover $\mathbb{Z}^n$. A lattice Λ is a *lattice packing (tiling)* with the shape $\mathcal{S}$ if Λ forms a packing (tiling) with $\mathcal{S}$. The following lemma is well known.

Lemma 1: A necessary condition that the lattice Λ defines a lattice packing (tiling) with the shape $\mathcal{S}$ is that $V(\Lambda) \geq |\mathcal{S}|$ ($V(\Lambda) = |\mathcal{S}|$), where $|\mathcal{S}|$ denote the volume of $\mathcal{S}$.

A linear code $\mathcal{C}$, over $\mathbb{Z}_q^n$, which corrects t asymmetric errors with limited-magnitude ℓ viewed as a subset of $\mathbb{Z}^n$ is equivalent to an integer lattice packing with the shape $\mathcal{S}(n,t,\ell)$. Therefore, we will call this lattice a *lattice code*.

Let $\mathcal{A}(n,t,\ell)$ denote the set of lattice codes in $\mathbb{Z}^n$ which correct t asymmetric errors with limited-magnitude ℓ. A code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ is called *perfect* if it forms a lattice tiling with the shape $\mathcal{S}(n,t,\ell)$.

Let $[\ell]$ be the set $\{0,1,2,...,\ell\}$ and let G be an Abelian group. A $\mathcal{B}_h[\ell](G)$ sequence of length m is a sequence (set) of m elements in G, $b_1, b_2, ..., b_m$ ($\{b_1, b_2, ..., b_m\}$) such that all sums

$$\sum_{j=1}^{m} \alpha_j b_j \ ,$$

where $\alpha_j \in [\ell]$ and at most h of the the α_j's are nonzero, are distinct elements of G. $\mathcal{B}_h$ sequences were first mentioned in [6] for correction of asymmetric errors with limited-magnitude.

Lemma 2: If $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ then there exists an Abelian group G of order $|G| = V(\mathcal{L})$ and a $\mathcal{B}_t[\ell](G)$ sequence of length n.

Lemma 3: Let G be an Abelian group and let $b_1, ..., b_n$ be a $\mathcal{B}_t[\ell](G)$ sequence. Then there exists a lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ with $V(\mathcal{L}) \leq |G|$.

Corollary 1: A perfect lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ exists if and only if there exists an abelian group G of order $|\mathcal{S}(n,t,\ell)|$ and a $\mathcal{B}_k[\ell](G)$ sequence of length n.

To form a code $\mathcal{C} \subseteq \Sigma^n$, where $\Sigma \stackrel{\text{def}}{=} \{0,1,\ldots,\sigma-1\}$, which corrects t asymmetric errors with limited-magnitude ℓ, one can take a lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$. Then $\mathcal{C} \stackrel{\text{def}}{=} (X + \mathcal{L}) \cap \Sigma^n$, where X is any element of $\mathbb{Z}^n$ added to all the elements of the lattice $\mathcal{L}$, is an appropriate code. Note that the code $\mathcal{C}$ is usually not linear.

III. Perfect Codes which Correct $n-1$ Errors

To use Corollary 1, we have to compute $\mathcal{S}(n,t,\ell)$.

Lemma 4: $|\mathcal{S}(n,t,\ell)| = \sum_{i=0}^{t} \binom{n}{i} \ell^i$.

Corollary 2: $|\mathcal{S}(n,n-1,\ell)| = (\ell+1)^n - \ell^n$.

For the ring $G = \mathbb{Z}_q$, the ring of integers modulo q, let G^* be the multiplicative group of G formed from all the elements of G which have multiplicative inverses in G.

Lemma 5: Let $n \geq 2$, $\ell \geq 1$, be two integers and let G be the ring of integers modulo $(\ell+1)^n - \ell^n$, $\mathbb{Z}_{(\ell+1)^n - \ell^n}$. Then,

(P1) ℓ is an element of G^*.

(P2) The element $x = (\ell+1) \cdot \ell^{-1}$ of G is an element of G^* of order n.

(P3) The expression $1 + x + x^2 + ... + x^{n-1}$ equals to *zero* in G.

(P1) and (P2) are important in the construction obtained from the following theorem, while (P3) is important for its proof.

Theorem 6: For each $n \geq 2$ and $\ell \geq 1$, let $x = (\ell+1) \cdot \ell^{-1} \in \mathbb{Z}^*_{(\ell+1)^n - \ell^n}$. Then the set $\{1, x, x^2, ..., x^{n-1}\}$ is a $\mathcal{B}_{n-1}[\ell](\mathbb{Z}_{(\ell+1)^n - \ell^n})$ sequence.

Corollary 3: For each $n \geq 2$ and $\ell \geq 1$ there exists a perfect lattice code $\mathcal{L} \in \mathcal{A}(n, n-1, \ell)$.

IV. Nonexistence of some Perfect Codes

Recall that there exists a perfect lattice code $\mathcal{L} \in \mathcal{A}(n,t,\ell)$ for various parameters with $t=1$. Such codes also exist for $t=n$ and all $\ell \geq 1$ and for the parameters of the Golay codes and the binary repetition code of odd length. In Section III we proved the existence of such codes for $t = n-1$ and all $\ell \geq 1$. Next, we ask whether such codes exist for $t = n-2$? Unfortunately, if $t = n-2$ and $\ell = 1$ such codes cannot exist. The proof is based on the following lemma.

Lemma 7: If there exists a perfect lattice code in $\mathcal{A}(n, n-2, l)$ then $|\mathcal{S}(n, n-2, \ell)|$ divides $(\ell+1)^{n-2} \cdot (\ell+1+\alpha \cdot (n-2-\ell))$ for some integer α, $0 \leq \alpha \leq \ell$.

Theorem 8: There are no perfect lattice codes in $\mathcal{A}(n, n-2, 1)$ for all $n > 3$.

V. Conclusion

We discussed three different equivalent ways to consider linear codes which correct t asymmetric errors with limited-magnitude ℓ. One of these ways was to consider $\mathcal{B}_h$ sequences. We presented a construction of $\mathcal{B}_h$ sequences which result in perfect codes of length n for correction of $n-1$ asymmetric errors with limited-magnitude ℓ for any given ℓ. A related nonexistence result for $n-2$ errors and limited-magnitude one was given. It is a major research problem to prove whether more such perfect codes exist.

VI. Note Added

After the Arxiv submission we became aware of the work in [7] which contains Theorem 6.

Acknowledgment

This work was supported in part by the Israel Science Foundation (ISF), Jerusalem, Israel, under Grant No. 230/08.

References

[1] R. Ahlswede, H. Aydinian, and L. Khachatrian, “Unidirectional error control codes and related combinatorial problems”, in Proc. *Eighth Int. Workshop Algebr. Combin. Coding Theory (ACCT-8),* St. Petersburg, pp. 6–9, 2002.

[2] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, “Codes multi-level flash memories: correcting asymmetric limited-magnitude limited-magnitude errors”, in Proc. *IEEE Inter. Symp. on Inform. Theory,* Nice, pp. 1176–1180, 2007.

[3] Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, “Codes for asymmetric limited-magnitude errors with application to multi-level flash memories”, *IEEE Trans. Inform. Theory*, vol IT-56, pp. 1582–1595, 2010.

[4] L. Dolececk, “Towards longer lifetime of emerging technologies using number theory”, in Proc. *Workshop on the Application of Commun. Theory to Emerging Memory Technologies*, Miami, pp. 1936–1940, 2010.

[5] N. Elarief and B. Bose, “Optimal, systematic, q-ary codes correcting all asymmetric and symmetric errors of limited magnitude”, *IEEE Trans. on Inform. Theory,* vol IT-56, pp. 979–983, 2010.

[6] T. Kløve, B. Bose, and N. Elarief, “Systematic single limited magnitude asymmetric error correcting codes”, *IEEE Trans. Inform. Theory*, vol IT-57, pp. 4477–4487, 2011.

[7] T. Kløve, J. Luo, I. Naydenova, and S. Yari “Some codes correcting asymmetric errors of limited magnitude”, *IEEE Trans. Inform. Theory*, vol IT-57, pp. 7459–7472, 2011.

[8] T. R. N. Rao and E. Fujiwara, *Error-Control Coding for Computer Systems*, London, U.K.: Prentice-Hall, 1989.

[9] M. Schwartz, “Quasi-cross lattice tilings with applications to flash memory,” in Proc. *IEEE inter. Symp. on Inform. Theory*, Saint Petersburg, pp. 2133–2137, 2011.

[10] S. Stein, “Tiling, packing, and covering by clusters”, *Rocky Mountain J. Math.*, vol. 16. pp. 277–321, 1986.

[11] E. Yaakobi, P. H. Siegel, A. Vardy, and J. K. Wolf, “On codes that correct asymmetric errors with graded magnitude distribution”, in Proc. *IEEE Inter. Symp. on Inform. Theory,* Saint Petersburg, pp. 1021–1025, 2011.